REPORT 2019

Sexualized violence online

Better protect children and young people from sexual assaults and abuse

JUGENDSCHUTZ.NET

IMPRINT

Contact
jugendschutz.net
Wallstraße 11
55122 Mainz, Germany
Tel: +49 6131 328520
buero@jugendschutz.net
www.jugendschutz.net

Authors
Melanie Giertz, Andreas Hautz,
Andreas Link, Jasmin Wahl

Translation
Jennifer Lopes

Responsible
Stefan Glaser

Graphic design
elements of art

as of
December 2019

jugendschutz.net has a legal mandate and is the German center at federal and state level concerning the protection of minors on the internet.

Better protect children and young people from sexualized violence on the internet

Depictions of child sexual abuse, sexual harassment and grooming: Unfortunately, there is a broad range of sexual assaults on children and young people on the internet. Additionally, the number of cases jugendschutz.net has to deal with explodes. Meanwhile our hotline receives nearly 40,000 reports concerning child sexual abuse material per year.

Sexualized violence starts as soon as the boundaries of sexual self-determination are overstepped. This is not only the case when a criminal offence has been committed, such as images or videos of child sexual abuse. If young people experience unwanted sexual approaches by strangers or someone they know on social media, e.g. through private messages, and if users post sexual comments to 'everyday photos' of children, this also violates the personal integrity of those concerned.

This report of jugendschutz.net gives an indication of the alarming scale of the phenomenon and shows us the need for urgent action. We specifically have to call providers of services popular with children and young people to account. Not only must they take swift action when it comes to infringements of the law, but also prevent sexualized violence against children. This includes implementing modern recognition tools to ban the dissemination of such material. An appropriate care pathway also comprises the protection of children's and young people's privacy, e.g. by providing safe default settings.

Finally, closer cooperation between national and international actors is essential: child and youth protection, law enforcement, politics, providers, science and education have to join efforts and develop comprehensive strategies to combat sexualized violence against children and young people online.

Stefan Glaser
Head of jugendschutz.net

CONTENTS

DANGERS AND RISKS

Sexualized violence against children and young people has a large presence online. It includes the sale of children as sex objects, solicitation of children for sexual purposes or unwanted dissemination of 'sexting' content they themselves generated.

Studies show that many minors have already personally experienced sexual harassment online. The risk increases with age and as soon as they move more freely on the internet. In popular online games and on services like WhatsApp, Instagram and YouTube, perpetrators actively seek to make sexual contacts with children and teenagers. Here, they continuously adapt their strategies to tie in with young people's online behavior and their living environment.

Sexual assaults can be deeply disturbing and can have negative effects on those concerned. The memorialization of the abuse through the production of photos or videos and knowing of the circulation of this material can substantially expand the harm. Witnessing the sexual harassment of others can also have a negative impact and make assaults seem acceptable. Young users can go on and become perpetrators themselves or no longer fight back.

Mass distribution of child sexual abuse images

Modern communication technologies make it easier than ever to document, distribute and access sexualized violence committed against children and teenagers. For example, the act can take place in Germany, the images or videos can be hosted on an American server, and accessed and further distributed by persons in very different countries.

The number of reports on child sexual abuse online has increased significantly over the last years. In 2018, jugendschutz.net received 39,500 reported URLs, compared with 4,300 URLs in 2016. Very often, it is also about the same depictions disseminated again and again. Automated systems of global players and hotlines analyze and identify thousands of already known depictions on a daily basis.

Project Arachnid (Canadian Centre for Child Protection) identifies known depictions of URLs reported. (Source: lollipoptakedown.ca)

Dissemination, procurement and possession of child and youth pornography is prohibited in Germany (cf. Sections 184 b and c of the German Criminal Code – StGB).

Additionally, tele media content depicting child sexual exploitation is illegal (cf. Article 4 (1) No. 9 and 10 of the Interstate Treaty on the Protection of Minors – JMStV).

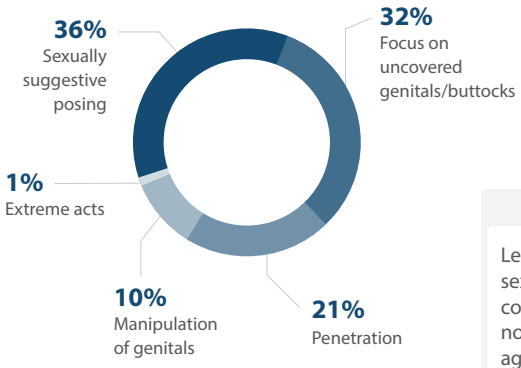
Furthermore, the creation and dissemination of voyeuristic depictions like e.g. secretly taken photographs in showers, restrooms or changing rooms violate a person's intimate privacy (cf. Section 201a of the German Criminal Code - StGB).

Photos and videos show various forms of sexualized violence

Depictions of sexualized violence against children and young people circulate on the internet in all kinds of different forms. They show e.g. explicit sexual acts, sexually suggestive posing or secretly filmed intimate moments in a voyeuristic manner and even depict the abuse of babies and toddlers.

jugendschutz.net regularly records vaginal, anal and oral penetrations as well as extreme sexual acts including animals. Realistic computer-generated images that are difficult to distinguish from natural images as well as textual descriptions of sexualized violence against children and young people are also disseminated online.

For creating sexualized depictions of children in suggestive poses, perpetrators stage them as sex objects: body posture, clothing, accessories and styling have a sexual connotation. Children pose in front of a camera, for example, in see through underwear, with handcuffs or making sexual gestures or suggestive body movements. Here, the camera's specific perspective lets the viewer think the child is sexually available or it meets voyeuristic preferences.



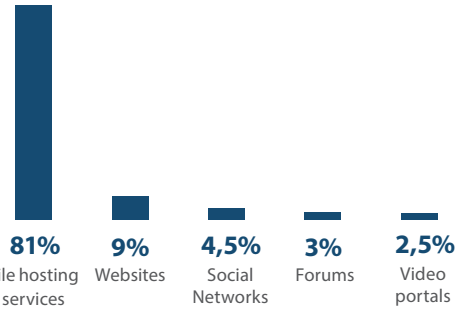
(Source: jugendschutz.net, 2018)

Legislation concerning depictions of sexualized violence differ from country to country. They do not always cover all phenomena known, and they also use different age limits as a basis. Generally, they ban depictions showing sexual activities with children younger than 13 years.

Sexualized violence against children as a business model

Depictions of sexualized violence against children and young people are not only accessible in hidden areas of the internet like in peer-to-peer networks or in dark net forums. jugendschutz.net's research shows that child sexual abuse material is also easily available and distributed via a large number of services in the World Wide Web.

Most of these are hosted abroad (87 %) and made available through so-called file hosting services (81 %). Specifically image hosting services allow users to upload photos to a centralized file storage free of charge, to have access anytime and integrate the photos in other websites. The services' content guidelines explicitly prohibit the disseminating of child sexual abuse material. However, perpetrators still exploit the platforms for exactly this reason.



Dissemination of child sexual abuse material via these services
(Source: jugendschutz.net, 2018)

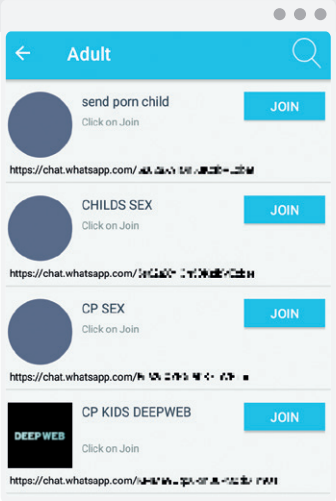
2018
Predominant use of servers in RU, NL, USA.

When it comes to the dissemination of depictions of sexualized violence, commercial aspects also play a role. Image hosting services, for instance, offer users uploading the images the chance to make money with child sexual abuse material by being paid by clicks. There are also portals providing a member's area with a payment system for more abuse content and even websites making abuse available upon request and against payment. Here, users can pay to watch live webcam child sexual abuse and sometimes even give instructions for the abusive acts.

Social Media serves as a hub for pedosexuals to network and trade

Even popular social media networks like Tumblr, YouTube and Instagram play a role when it comes to disseminating depictions of sexualized violence. Persons with a sexual interest in children use all the services' functions to find and connect with each other. They like, share, follow content and post comments to show their mutual interest in child sexual abuse content, and use private messages to get in touch.

Contrary to the social media principle of gaining as many followers as possible, the aim here is to address the 'right' users. Very often, typical keywords and abbreviations or images of already known victims serve as identifying features. In many cases, pedosexuals move their communication to private groups or other services to avoid being detected and removed from the platform.



WhatsApp groups with explicit names. (Source: Group links for WhatsApp)

On the popular messaging service WhatsApp, jugendschutz.net identified groups for exchanging depictions of sexualized violence with users numbering in a three-digit range. In this case, not only insiders could gain access to the content. Perpetrators used public advertising portals like 'Group Links for WhatsApp' to promote the groups. Publicly available information like names and/or profile pictures were clear indications of child sexual abuse content.

Like-minded users find each other on popular platforms.

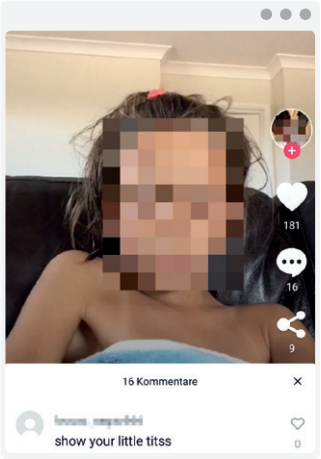
Insufficient precautions by providers contribute to sexual harassment and online grooming

According to EU Kids Online, 34 % of all girls and 23 % of all boys interviewed in Germany have been faced with intimate or suggestive questions they did not want to answer. These range from questions about their sexual experiences and preferences to invitations to engage in sexual activities (Results of the EU online survey in Germany in 2019 on 'online experiences of 9- to 17-year-olds').

Sexual harassment of children and young people mainly takes place in services that also address adults and offer private communication features next to public ones like on social media and in online games. Many of these have no sufficient moderation and/or have default settings that do not adequately protect young users' privacy. This makes the risk particularly high.

By default, TikTok accounts are public, which allows anyone to view a user's profile and uploaded videos and any logged in user can post comments. TikTok requires a minimum age of 13 years to sign up. However, there are plenty of younger children presenting themselves on self-recorded videos.

jugendschutz.net documented a large number of harassing comments and direct invitations to engage in sexual activities like '…you all know this moment when you just want to stick it in' or 'you served as my jerk-off model'. Adults also tried to get in contact with minors and move the communication to other services with private chat features like WhatsApp or Snapchat.



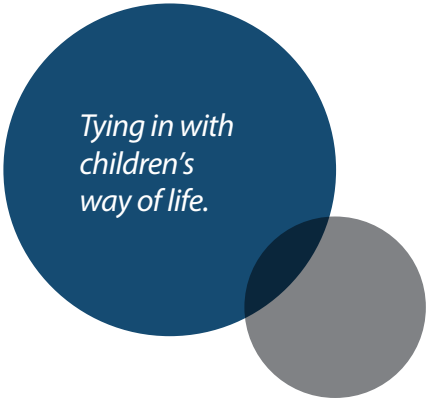
Request to a young TikTok user to show more of herself. (Source: TikTok; original not pixelated)

Children and young people often disclose private information unintentionally, post links to profiles on Snapchat and YouTube that everyone can see or share their current location in their Instagram posts. This puts them at risk of being identified by strangers and being exposed to assaults even offline.

Equally, online games like 'Clash of Clans' or 'Minecraft' are platforms for perpetrators to facilitate online grooming. Repeatedly, there are cases where they exploit chat features to get in touch with minors. They try to build trust gradually through joint activities in the game. This can even happen in communities particularly designed for children as a recent case in Austria demonstrated. A 36-year-old man pretended to be a 13-year-old boy and used the MovieStarPlanet app to get in contact with girls aged between 11 and 15 years resulting in sexual assaults offline.

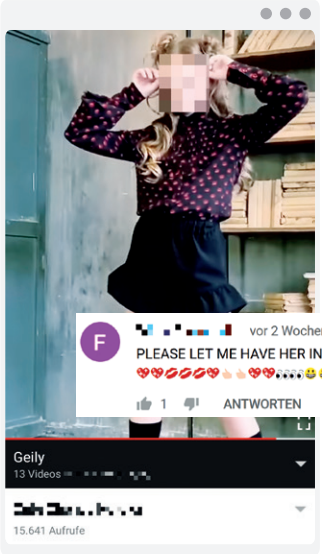
Online grooming is the process by which someone befriends and gains the trust of a child for sexual purposes online or offline. Perpetrators intentionally tie in with young people's interests and needs in order to persuade them to perform sexual acts in front of their webcam or to prepare a sexual abuse in real life. Very often, there was overlapping with phenomena such as sexual harassment and/or sextortion, using intimate recordings for blackmailing.

In accordance with Section 176 (4) No. 3 of the German Criminal Code – StGB, online grooming is criminalized as a special form of child sexual abuse. Corresponding actions towards young people aged 14 to 18 are not part of this legislation. Online grooming is often only defined as such in retrospect after an abuse in real life.



‘Everyday images’ of children exploited for sexual purposes

Images and videos of children during everyday activities, on the playground, at the beach or doing sports are also exploited online for sexual purposes. Pedosexuals share them on pornographic websites, post sexual comments to them in social networks or create favorites and playlists (a collection of videos) with sexualized titles. However, everyday images of children are also available in profiles and forums specifically used for disseminating child sexual abuse material.



Video showing a girl dancing; added to the explicit playlist ‘Geily’ with sexual comments. (Source: YouTube; original not pixelated)

jugendschutz.net recorded sexual comments especially to gymnastics and bathing videos of children on YouTube. Sometimes the comments led the way to scenes showing children spreading their legs. On top of that, YouTube’s recommendation algorithm even suggests more related videos.

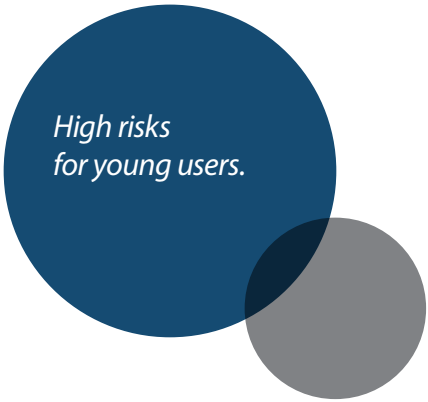
YouTube announced to disable comments on videos featuring children and to introduce new rules restricting children from live streaming. In the end of 2019, YouTube also faced criticism because of playlists. funk, a public service content-network for teenagers and young adults provided by the TV channels ARD and ZDF, called attention to a compilation of ‘everyday videos’ with sexualized titles and emphasized pedosexuals’ networking and manipulation strategies.

In legal terms, the phenomenon of sexualized ‘everyday images’ is a grey area. Posting such images is not illegal. Parents and children often post the images themselves. However, misuse by adding sexualizing elements is not completely covered by legislation although it violates children’s privacy and suggests their sexual availability.

Users disseminate private ‘sexting’ photos without prior consent

Creating and sending self-generated explicit images – sexting – is increasingly common among young people today. They exchange revealing photos and videos for flirting or for sexual arousal. However, again and again and ‘just for fun’ or out of revenge, these are posted publicly or disseminated among peers or at school without the consent of the individual appearing in the photo. Depending on the age, this can constitute the criminal offence of dissemination, procurement and possession of child or juvenile pornography; even if it is done without thinking.

Once online, this content often circulates endlessly on the internet. Repeatedly, users share and re-upload the images. For those affected, this can cause psychological distress and additionally come along with blackmailing (sextortion) or systematic cyberbullying and exclusion. In fact, there have already been recent occasions where students had to leave the school because of nude pictures of them posted to a class WhatsApp group.



Next to WhatsApp, Snapchat is also popular for sexting. Allegedly, Snapchat enables safe sexting: Private messages can only be seen to a maximum of two times, after that they self-destruct automatically. However, Snapchat users can take screenshots to save and further disseminate content and images. There are collections of images posted without the individuals in the pictures knowing about it.

COUNTER STRATEGIES AND PROTECTION

The many different forms of sexualized violence against children and young people online call for close collaboration between national and international players.

In terms of depictions of child sexual abuse, quick removal has been paramount. However, best practice actions seems to have reached its limits given the sheer volume of content disseminated. In order to take proactive measures to prevent the dissemination of this content, providers must implement effective protection systems. In addition to age-appropriate default settings and functional reporting systems, they should also use technical mechanisms that already today are able to recognize child sexual abuse content very reliably.

Some areas of sexualized violence are not brought within the whole scope of criminal law, e.g. sexual commenting to 'everyday images' and verbal sexual harassment. This, however, also puts young people's personal integrity at risk or degrades and objectifies them for the sexual pleasure of adults. Here, the legislative framework must be adapted.

In order to make young people more aware of the dangers of sexualized violence, parents, guardians and teachers need information and tips for a risk management for different ages.

Remove content and identify perpetrators

jugendschutz.net achieved removal of more than 90 % of all child sexual abuse content identified in 2018. In terms of content hosted on German servers, it took an average of 3.5 days to have it removed; content hosted abroad was removed within 7 days.

When it comes to combating child sexual abuse material, jugendschutz.net collaborates closely with the German Federal Criminal Police Office (BKA), the hotlines eco (Association of the Internet Industry), FSM (German Association for Voluntary Self-Regulation of Digital Media service providers) and the BPjM (Federal Review Board for Media Harmful to Minors). jugendschutz.net forwards content that is punishable under the criminal code and hosted on German servers to the BKA for further investigations. After collecting evidence, the BKA then calls on providers to remove the content.

At international level, jugendschutz.net cooperates with INHOPE (International Association of Internet Hotlines) consisting of hotlines from more than 40 countries. A common database allows for a quick exchange of reports. This database is coupled with INTERPOL's International Child Sexual Exploitation database, which relies on hash values enabling automated recognition of known images and videos. It filters unknown material and forwards it to law enforcement to support victim and perpetrator identification.

A report from Germany helped the Danish police identify victim and perpetrator within a short period. The website reported contained videos of a sexually abused child available for download. Uploading the video to the INHOPE database and classifying the content enabled INTERPOL's investigators to track the GPS data and pinpoint the crime scene. Within just a few hours, the Danish police officers could identify the perpetrator and rescue the child victim.

A report from Germany also resulted in another arrest in Austria. jugendschutz.net's research in the field of naturism online revealed a website disguised as a naturist site. In the preview area, however, the website presented children in sexually suggestive poses and even professionally promoted the content in a member's area. jugendschutz.net informed the Austrian hotline and the Austrian Federal Criminal Police Office and provided more evidence which eventually led to the arrest of the website owner.

Effectively combat illegal structures and obligate providers to take precautions

Successfully combating sexualized violence against minors on the internet calls for more efforts than just removing single items. The phenomenon needs a systematic approach and has to be seen as a whole in order to develop sustainable counter strategies.

Effectively combating child sexual abuse material online needs analysis of typical distribution channels, the perpetrators' network and their cover-up strategies. This structural knowledge helps implement and coordinate measures to identify perpetrators, protect victims, remove content and proactively prevent further dissemination.

In addition, there is a need for taking a close look at all forms in the grey area of child sexual abuse like depictions of girls or boys in sexually suggestive poses and 'everyday images' of children. Adults specifically use this kind of content as a 'teaser' for exchanging and consuming more extreme images of child sexual abuse. They blur the legal lines and play down sexualized violence. There is only one way of preventing this: Any kind of sexualization of children has to be banned and punished consistently.

Sexual harassment and online grooming have their own way. Next to young users' inexperience and credulity, pedosexuals especially exploit safety gaps in services that are specifically attractive to children and young people. Here, they are unguarded and perpetrators can easily get in contact with them. It is imperative to check these gateways on a regular basis and call on providers to improve their protection systems.

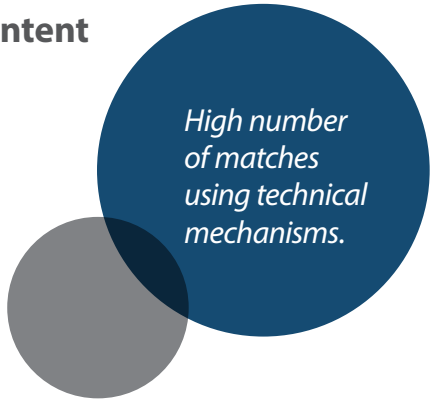
Operators of services that are popular among children and young people have to be obliged to take precautions. When designing their content, they have to provide access for young users appropriate to their age, in accordance with the principle of Safety by Design. This reduces the risk of sexual assaults and the confrontation with inappropriate sexualized content.

When under 18-year-olds sign up, default settings should prevent their personal information like e.g. their current location or contact details, from being publicly available. Use of communication features should be restricted to trustworthy persons, friends or friends of friends in order to prevent unwanted contacts.

Additionally, there is a need for support tailored to the target group. This can help teach young users how to behave safely online and make them aware of risks. Helplines like the 'Nummer gegen Kummer' and the 'Sexual Abuse Telephone Helpline' also offer guidance and support in sexual abuse cases. They should be easy to find and easy to access and use.

A precautionary approach must include easy accessible, easy to use and effective reporting options for content depicting sexualized violence. Quick removal of such content is especially important to protect the victims and prevent further dissemination of the traumatizing content.

Implement technical measures for combating child sexual abuse content and make these more effective



Given the growing proliferation of child sexual abuse material online, the use of automated recognition systems is also key when it comes to combating this content. For years now, hash functions have been able to recognize known images very reliably by creating a hash of a file, just like a digital fingerprint. Major platforms as Google and Microsoft already use hash algorithms to prevent re-upload of already known child sexual abuse images.

The Dutch INHOPE partner hotline EOKOM provides a so-called hash check service to help hosting providers and website owners to prevent the spread of online child sexual abuse material. This enables them to check hashes of images with a database of more than a million hashes before uploading images and thus prevents re-upload of content that has already been assessed as illegal. In the United Kingdom, forums and platforms are checked for matches with a hash list compiled by the Internet Watch Foundation (IWF) and providers are put on notice.

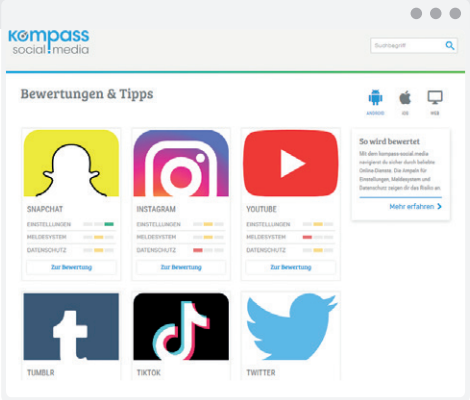
Project Arachnid, developed by the Canadian Center for Child Protection, shall help hotlines automate the processing of reports. Arachnid recognizes depictions of child sexual abuse on a website reported – here also by comparing the image displayed to a hash database. Fully automated, the next steps include a notice to law enforcement, providers and/or partner hotlines concerned. In a trial phase, jugendschutz.net is currently participating in Project Arachnid to see how it fits into the hotline work and can improve the effectiveness in Germany.

Artificial Intelligence is considered very promising when it comes to recognizing unknown child sexual abuse images. It is based on the principle of learning algorithms trained with large amounts of data. It recognizes patterns and transfers these to unknown material. Such instruments can be a substantial improvement to the approach towards fighting child sexual abuse images and can provide support to law enforcement.

Support and enable children and young people to protect themselves

The protection of children and young people from sexualized violence online needs media educational support. It is unrealistic to expect to prepare them for all possible situations. Therefore, the prime objective has to be to introduce them to interactive online content according to their age. Here, tips for communicating safely online are very helpful. They should be encouraged to turn to a person they trust whenever they feel uncomfortable.

Because of their specific need for protection, children require safe content online to familiarize themselves with the internet and learn the right skills. When it comes to teenagers, sexual experiences online are very common. They need help to increase their self-confidence and bodily self-awareness in order to recognize sexual assaults and set limits.



kompass-social.media: Evaluation of risks & tips for behaving safely on popular platforms.
(Source: jugendschutz.net)

Behaving safely online includes disclosing as little personal data as possible and a critical reflection of how to present oneself. jugendschutz.net provides online information on risks on social media and tips on how to teach media literacy.

Safe participation through media competence and age-appropriate risk management.

Allow children and young people to grow up well in a digital world

As the German center at federal and state level concerning the protection of minors on the internet, jugendschutz.net looks closely at risks in internet services specifically attracting young people and urges providers and platform operators to design their content in a way that allows children and young people to use the internet free of troubles.

jugendschutz.net operates a hotline accepting reports about content violating youth protection laws.

Internet users can report unlawful content to:
www.jugendschutz.net/hotline

JUGEND SCHUTZ.NET